Information Technology Executive Council (ITEC)

ITEC Policy 7320A

Enterprise IT Security Reporting Protocols

Enterprise IT Security Reporting Protocols

October 24, 2007

Purpose

These protocols are put forth to help the KANWIN network maintain availability, integrity and confidentiality and to document, authorize and establish continuing incident handling management standards, disciplines and processes across the enterprise. Incorporated within these protocols are accepted best practices within the law enforcement and IT security communities. These procedures will facilitate cooperation and information exchange among all KANWIN users, who are responsible for reporting on, and responding to, cyber security incidents.

References

Kansas Information Technology Executive Council (ITEC), ITEC Policy 7300, Information Technology Security Council Charter.

ITEC policy 7230 A, General Information Technology Enterprise Security Policy.

Department of Administration Intrusion Detection Incident Response Security Policy and Procedure.

National Institute of Standards and Technology Special Publication 800-61 “Computer Security Incident Handling Guide”

Carnegie Mellon University Software Engineering Institute “Handbook for Computer Security Incident Response Teams (CSIRTs)”

USDA Cyber Security Incident Handling Procedures manual (March 20, 2006)

Forum of Information Response and Security Teams (FIRST) http://www.first.org/resources/guides/csirt_case_classification.html (November 17, 2004)

Central Point of Contact: Enterprise Security Office (ESO) (tel # 785-296-0814)

Security Incident Definition: Compromise of any system that has critical, sensitive, or confidential data, or any compromise that significantly affects entity resources or,

The act of violating an explicit or implied security policy

The act of violating any Federal, State or local law

These activities include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data

- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Security Incident Thresholds

Security incidents may be considered as such when certain conditions are met. Guidelines as to thresholds of actions and reporting may be considered when the following parameters are present either all or in combination.

- Six or more machines per LAN segment showing IPS signature trigger over 15 minutes time.
- Six or more machines showing IPS signature triggers of over 10 events per minute.
- One or more machines identified as critical infrastructure/applications/business units.
- Significant impact on bandwidth for 30 minutes.
- When a concerted effort is shown to be attacking the network either internally or externally.
- Any known or reported compromise of Personal Identifiable Information (PII).
- Any entity website defacement.

Security Incident Categories

All incidents managed by the ESO Computer Security Incident Response Team (CSIRT) should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	♦ DOS or DDOS attack.
Compromised Information	S1	♦ Attempted or successful destruction, corruption, or disclosure of sensitive state information or Intellectual Property.
Compromised Asset	S1, S2	♦ Compromised host (root account, Trojan, root kit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	♦ Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	♦ Reconnaissance or Suspicious activity originating from inside the KANWIN network, excluding malware.

External Hacking	S1, S2, S3	♦ Reconnaissance or Suspicious Activity originating from outside the KANWIN network, excluding malware.
Malware	S3	♦ A virus or worm typically affecting multiple entity devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	♦ Fraudulent email.
Policy Violations	S1, S2, S3	♦ Sharing offensive material, sharing/possession of copyright material. ♦ Deliberate violation of Information security policy. ♦ Inappropriate use of state asset such as computer, network, or application. ♦ Unauthorized escalation of privileges or deliberate attempt to subvert access controls.
* Sensitivity will vary depending on circumstances		

Criticality Classification

The criticality matrix defines the minimal customer response time and ongoing communication requirements for a case. The criticality level should be entered into the Incident Tracking System (ITS) when a case is created, and it should not be altered at any point during the case lifecycle except when it was initially incorrectly classified. Typically the Incident Manager (IM) will determine the criticality level. In some cases it will be appropriate for the IM to work with the customer to determine the criticality level.

Criticality Level	Criticality Level Definition	Typical Incident Categories	Initial Response Time	Ongoing Response (Critical Phase)	Ongoing Response (Resolution Phase)	Ongoing Communication Requirement
1	Incident affecting critical systems or information with potential to have revenue or customer impact	♦ Denial of service ♦ Compromised Asset (critical) ♦ Internal Hacking (active) ♦ External Hacking (active) ♦ Virus / Worm/Bot (outbreak) ♦ Destruction of property (critical)	60 Minutes	CSIRT Incident Manager assigned to work case on 24x7 basis.	CSIRT Incident Manager assigned to work on case during normal business hours.	Case update sent to appropriate parties on a daily basis during critical phase. If CSIRT involvement is necessary to restore critical systems to service then case update will be sent a minimum of every 2 hours.
2	Incident affecting non-critical systems or information, without revenue or customer impact (Employee investigations that are time sensitive should typically be classified at this level)	♦ Internal Hacking (not active) ♦ External Hacking (not active) ♦ Unauthorized access. ♦ Policy violations ♦ Unlawful activity. ♦ Compromised information ♦ Compromised asset. (non-critical) ♦ Destruction of property (non-critical)	4 hours	CSIRT Incident Manager assigned to work case on 24x7 basis.	CSIRT Incident Manager assigned to work on case during normal business hours.	Case update sent to appropriate parties on a daily basis during critical phase. Case update sent to appropriate parties on a weekly basis during resolution phase.
3	Possible incident, non-critical systems. Incident or employee investigations that are not time sensitive. Long-term investigations involving extensive research and/or detailed forensic work.	♦ Email ♦ Forensics Request ♦ Inappropriate use of property ♦ Policy violations	48 Hours	Case is worked as CSIRT time/resources are available.	Case is worked as CSIRT time/resources are available.	Case update sent to appropriate parties on a weekly basis.

Definitions

Initial Response Time – This specifies the maximum amount of time that should elapse before a Computer Security Incident Response Team (CSIRT) Incident Manager responds to the customer. Again, this is the maximum amount of time. In most cases the IM will response sooner than the specified response time. At a minimum, the following should occur within this timeframe:

- Initial assessment and triage.
- Case classification is determined.
- The case will be entered into the ITS.
- The case ownership will be established. (Either the on-call IM will own the case, or it will be assigned to another IM).
- An email will be sent to the customer. This is the initial "we have your case" email. This email will include various information (to be defined in another document) such as the date/time of the request, ITS case number, the name, phone, and email of the incident manager, a CSIRT escalation contact, the criticality and sensitivity level of the case, and an indication of when the customer will receive case updates. Ideally, the ITS will generate this email automatically when a case is entered into the system.

Ongoing Response Requirement - This specifies the level of service that the customer will receive from the CSIRT.

Ongoing Communication Requirement – This specifies the frequency in which communications with the customer should occur throughout the case lifecycle. These are the minimum requirements, communications may occur more frequently as required. Incident Phases:

Incident Phase	Description	Typical Activities
Critical Phase	The period of time in the case lifecycle when active incident response is required in order to ensure the successful resolution of the case. Typically this includes system or service outages, and/or urgent evidence preservation.	Detection, assessment, triage, containment, evidence preservation, initial recovery
Resolution Phase	The period of time in the case lifecycle when active incident response is not required to successfully resolve the case.	Evidence collection, analysis and investigation, forensics, remediation, full recovery, post-mortem.
Notes: The ITS should include a notation for the incident phase ('Critical', 'Resolution', 'N/A'). For cases that are classified as C1 or C2 this notation would be set to Critical when the case is opened, and would be changed to 'Resolution' at the appropriate time in the case lifecycle. For cases that are not time-sensitive (typically C3) the IM would note field as 'N/A'. Having this distinction will allow CSIRT personnel and Security Operations management to easily distinguish between cases that are critical and active from those that are not being actively worked.		

Sensitivity Classification

CSIRT staff should always apply the "need to know" principle when communicating case details with other parties. The sensitivity matrix below helps to define "need to know" by classifying cases according to sensitivity level. The 'Required' column defines the parties that "need to know" for a given sensitivity level. The 'Optional' column defines the other parties that may be included on communications, if necessary. Typically the IM will determine the sensitivity level. In some cases it will be appropriate for the IM to work with the customer to determine the sensitivity level.

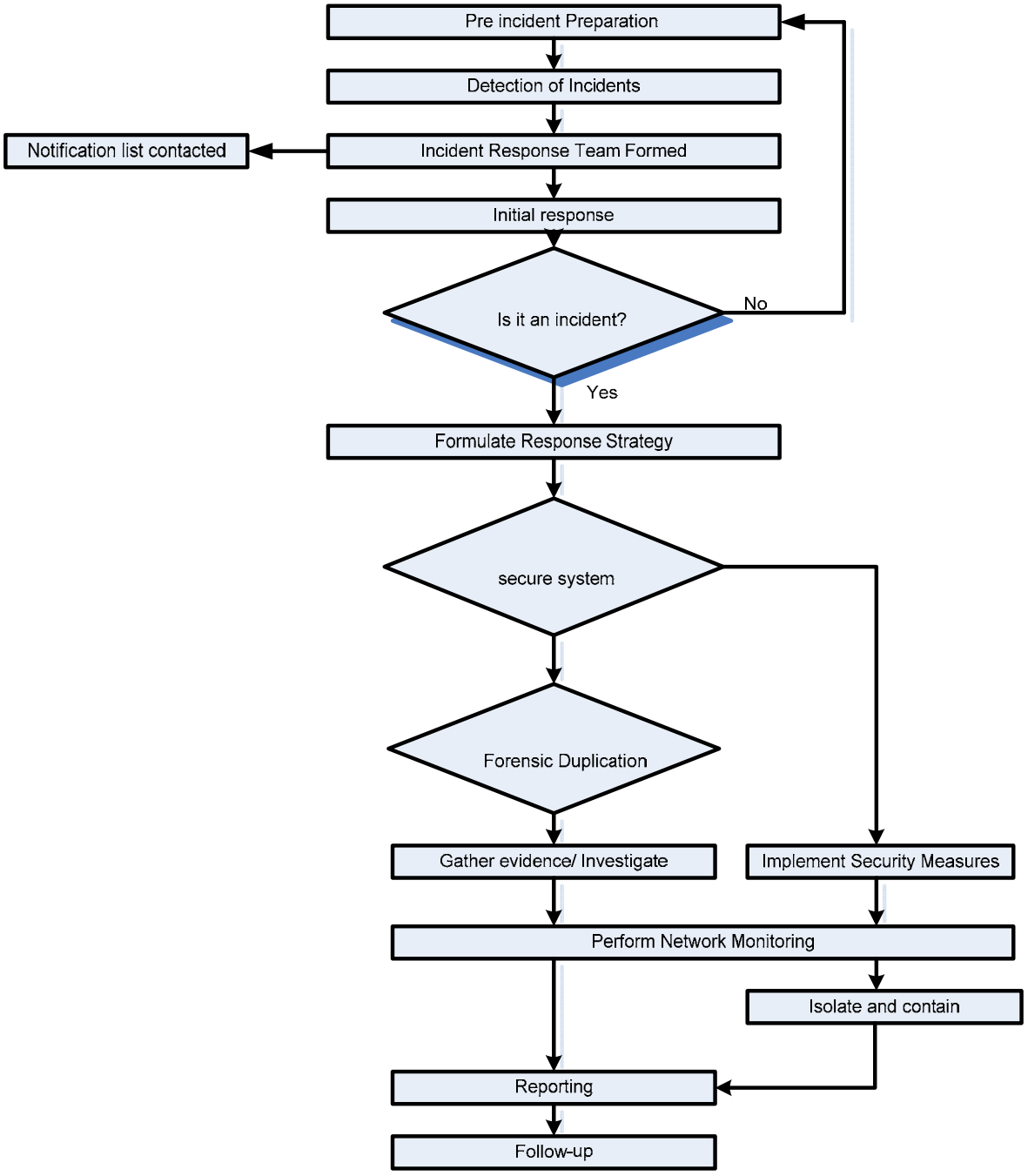
Sensitivity Level	Sensitivity Level Definition	Typical Incident Categories	Required On Case Communications **	Optional On Case Communications **	IT Staff Access
1	Extremely Sensitive	♦ Global Investigations Initiated. ♦ Forensics Request ♦ Destruction of property. ♦ Compromised asset. ♦ Compromised information. ♦ Unlawful activity. ♦ Inappropriate use of property. ♦ Policy violations	CSIRT	Entity security contact	CSIRT, Entity Security contact
2	Sensitive	♦ External Hacking ♦ Internal Hacking/ ♦ Unauthorized Access	CSIRT	Security Operations, OWNERS	Security Operations
3	Not Sensitive	♦ Denial of service. ♦ Virus / Worm ♦ Email	CSIRT	ANY	ALL Agents in ITS

Notes:

** "Case Communications" include the following: Initial email from CSIRT to customer, periodic case reports to customer, and final case report to customer. It is not necessary to include these parties on all interim communications that occur throughout the life of a case, only the case updates and summary.

Security Work Flow

Enterprise Security Office
Intrusion Detection Workflow Model



Security Incident-Related Contacts

Each entity should appoint an official security point of contact (POC) and a secondary POC to act as a liaison with the State Chief Information Security Officer. When the Security Officer discovers a security incident occurring in an entity, he or she will report the incident to the entity POCs. After reporting the incident to the POCs, the latter may also need to contact other officials or staff within the entity in order to investigate or respond to the incident.

Additional contacts from within the entity, from other entities, or externally may include the following:

- Upper management (managers, department/division/bureau heads)
- Sponsors
- Other departments
- Technical (system and network) administrators
- Security officers
- Legal counsel or legal compliance department
- Internal audit department
- Network control center (NCC)
- ISP operations center
- Security vendors

In large entities there may be a predetermined initial point of contact (POC) that is notified concerning an incident report occurring at that particular site. However, it may be essential after the initial POC to then be placed in contact with a specific department or other appropriate individual(s) who can respond to the activity.

Pre-registration of Contact Information

This process is to solicit information in advance from other parties, such as other entities. Such a registration process is to help prevent the need for standard questions to be handled on a case-by-case basis for every new report/request.

Pre-registered items include, for example:

- Trusted points of contact and associated contact information (must be routinely verified, at least once a year)
- Information disclosure restrictions (verified) keys for encrypted and/or signed exchange of information

Security Incident Notification Protocols

An Individual entity is notified for security incident thresholds items 1, 2, and 3 (page two)

Enterprise notification takes place for items 1 and 2 above (possibly 3)

Enterprise notification may consist of IT Security Council, ITAB, and/or the Security Users Group. Incident notification to the enterprise may also take place via email to an IT Security Broadcast List. The "who" to be notified will likely be dependent upon the nature of the incident and when it occurred.

During normal business hours, notification will most often emanate from the Enterprise Security Office (ESO). After hours, notification may be made by the DISC Network Control Center (NCC) or by the ESO after consultation with the Chief Information Security Officer (CISO).

Where it is determined or where there is reason to believe an incident involves Compromised Information or Unlawful Activity, or where it is anticipated the incident will result in a media release, immediate notification and consultation with the Department of Administration Legal will be effected, followed by notification of local law enforcement, the KBI, and the Attorney General.

Announcements

Announcements are generated with information tailored for the enterprise in various formats. The nature of announcements varies from disclosing details of ongoing threats and, steps taken to protect against those threats, to sanitized trend information on recent attacks reported to the ESO. Its function may be limited to its direct applicability with the incident handling service.

Announcement Types

Announcements can take on many forms, from those providing short-term information related to a specific type of ongoing activity to general long-term information for improving awareness and system security. The following are categories of announcement types:

"Heads-up"

The heads up process usually takes the form of a short message, issued when detailed information is unavailable. The purpose is to inform the enterprise or other parties of something that is likely to be important in the near future. Announcing a heads-up has multiple benefits. First, the ESO or CSIRT can proactively warn or inform their constituency to a potential issue or threat. Second, the recipients may already know something about (or have additional information relating to) an issue detailed in the heads-up than the ESO or CSIRT. This gives the constituency the opportunity to provide feedback to the team. Third, the recipients may stumble on information related to the content of the heads-up at some later time. They will then be in a better position to recognize the information and its potential importance. There is a caveat, however, that information in such documents is likely (and often expected) to change, so it might be worth including a disclaimer prominently in the text of the "heads up" to clearly identify when the information is unconfirmed or speculative.

Alert
Alerts are short-term notices about critical developments containing time-sensitive information about recent attacks, successful break-ins, or new vulnerabilities. There may already be complete information regarding the subject of an alert, but something may have changed to require the publication of new information.

Advisory
Advisories are often one of the most common documents produced by CSIRTs. Advisories provide mid-term and long-term information about problems and solutions suitable to raise awareness and help avoid incidents. They typically contain information about new vulnerabilities, but may also contain information about intruder activity. Advisories are often well researched and include substantial technical detail relating to patches and workarounds. Advisories are typically aimed at a technical audience such as system and network administrators, but sometimes contain additional background information for less technical readers. An example would be US-CERT Advisories.

For Your Information
These are documents that contain mid-term and long-term information, similar to advisories, but shorter and less technical to address a wider audience. These might be called briefs, bulletins, or newsletters as well. Such an announcement might typically contain information of a tutorial or instructive nature that can be used by non-technical personnel with an interest in security. This could include management or legal staff.

Guideline
A guideline is a sequence of steps that leads someone familiar with the basics of his craft through a process meant to expand that person's knowledge or even to work direct improvements (in system or network security). They can be lengthy documents aimed at helping technical staff improve their fundamental understanding of security and their day-to-day practices.

Entity/Organizational Reporting Responsibilities
Upon learning of or suspecting a cyber incident, entities are required to report information to the Enterprise Security Office by telephone at (785-296-0814) or via email to DAES_SecurityOffice@da.ks.gov with the subject line "Incident Notification" All known pertinent details should be conveyed to the ESO either verbally or via email. If log files are available they should be emailed to the DAES address.

In order to facilitate forensics investigation of the incident, no attempt should be made to examine the affected device(s). The steps in securing a computer device are as follows:

Secure the Computer as Evidence
- If computer is "OFF" do not turn "ON".
- If computer is "ON"
  - Stand-alone computer (non-networked)
  - Consult with an ESO security engineer

- If a security engineer is not available
  - Photograph the screen, then disconnect all power sources; unplug from the wall AND the back of the computer.
  - Place tape over each drive slot and mark “EVIDENCE”.
  - Photograph or diagram, then label back of the computer components with existing connections.
  - Label all connectors/cable ends to allow reassembly as needed.
  - If transportation is required, package components and transport/store components as fragile cargo.
  - Keep away from magnets, radio transmitters, and otherwise hostile environments.
- Networked or business computers
  - Consult the ESO for further assistance
  - Pulling the plug could:
    - Severely damage the system
    - Disrupt legitimate business
    - Create individual and department liability

Abbreviations

CIO	Chief Information Officer
CISO	Chief Information Security Officer
CITO	Chief Information Technology Officer
CS	Cyber Security
CSIRT	Enterprise Security Office Computer Security Incident Response Team
DNS	Domain Name Server
DoS	Denial of Service
ESO	Kansas Enterprise Security Office
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
I/D	Intrusion Detection
IDS	Intrusion Detection System
IM	Incident Manager
IP	Internet Protocol
IRT	Incident response team
ISP	Internet Service Provide
ISSP	Information Systems Security Program
IT	Information Technology
ITS	Incident Tracking System
KANWIN	Kansas Wide Area Information Network
POC	Point of Contact
SA	System Administrator
SOC	Security Operations Center
US-CERT	United States Computer Emergency Response Team
USSS	United States Secret Service

Definitions

Adverse event – An event that indicates or produces an actual or potential negative consequence to State of Kansas IT systems. This includes attempted or actual system crashes, network packet floods, unauthorized use or disclosure, defacement of a webpage, and execution of malicious code. [State of Kansas rates LOW and MEDIUM Intrusion Detection reports as undesirable events. High Intrusion Detection reports are to be considered CS incidents.] Documented and verified adverse events are incidents.

Adware – Any software application, which displays advertising banners while running a program. Adware includes additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on the computer screen. It usually includes code that tracks a user's personal information and passes it on to third parties without the user's authorization or knowledge.

Botnet – A network of compromised machines that can be remotely controlled by an attacker. Due to their immense size (tens of thousands of systems that can be linked together), they pose a severe threat to the Government's IT infrastructure.

Breach - Any illegal penetration or unauthorized access to a computer system that causes damage or has the potential to cause damage.

Chain of Custody - Protection of evidence by each responsible party to ensure against loss, breakage, alteration, or unauthorized handling. Protection also includes properly securing, identifying, and dating evidence.

Compromise –The unauthorized disclosure, modification, substitution, or use of sensitive information, or the successful action to invade system by evading its security. For example a computer has been compromised, when a Trojan horse has been installed.

Compromise of Integrity –Any unauthorized modification of information or data.

Cyber/Computer Security Incident – A violation or imminent threat of violation of computer security policies, acceptable uses or standard computer security policies. It is also any adverse event whereby some aspect of a computer system is compromised as: loss of data confidentiality; disruption of data integrity; disruption of availability, also known as a denial of service.

Damage –The unauthorized deliberate or accidental physical or logical modification, destruction, or removal of information or data from an IT system.

Denial of Service (DoS) – An inability to use system resources due to unavailability; for example, when an attacker has disabled a system, a network worm has saturated network bandwidth, an IP address has been flooded with external messages or the system manager and all other users become locked out of a system.

Event – Any observable or measurable occurrence in a system or network. Events may include, but are not limited to, a user connecting to a file share, a server receiving a

request for a Web page, a user sending electronic mail, and firewall blocking a connection attempt.

Finding – An event or occurrence that may cause a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

Firewall – A system that controls network traffic between two networks to minimize unauthorized traffic or access. Firewalls can protect networks and systems from exploitation of inherent vulnerabilities. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet.

Harm – To cause damage, injure or impair IT systems using electronic methods, which can include intangible things such as identity theft.

Incident Closure or Closeout – The last phase of incident handling lifecycle

Incident (Cyber Security) – A violation or imminent threat of violation of computer security policies, acceptable use or standard computer security practices. It is also any adverse event whereby some aspect of a computer system is compromised, such as loss of data confidentiality, disruption of data integrity, disruption, or denial of service. The types of incidents are been classified into LOW, MEDIUM or HIGH levels depending on the severity.

Incident Declaration – The phase of the incident handling lifecycle during which a State of Kansas incident number is assigned and the responsible State of Kansas organization begins its incident handling process. An incident is declared by a State of Kansas entity, staff, office, or Enterprise Security Office incident response team (IRT) the latter is recognized as being responsible for incident handling.

Incident Handling - The comprehensive management process of receiving incident indications and warnings from Intrusion Detection Systems (IDS), United States Computer Emergency Response Team (US-CERT), law enforcement or Internet Service Providers (ISP) that an incident has occurred. It includes identifying the actual incident type, verifying the victim or perpetrator's responsible entity, alerting the entity. It also requires reporting, responding to, mitigating, and closing a State of Kansas CS incident.

Incident Notification – This phase of the incident handling lifecycle involves the formal transmission of declared incident information to the documented incident handling or management personnel in the State of Kansas organization that is experiencing a CS incident.

Incident Oversight – The process of ongoing review and follow-up of incident status by the State of Kansas Enterprise IT Security Office, staff, or assignees to maintain accurate incident records on the number of incidents declared open, closed or cancelled. Statewide incident oversight is required for record keeping and review of closeout reports.

Incident Preparation – This phase of the incident handling lifecycle involves preparing reports and providing continuous status on the incident.

Incident Prevention – This phase of the incident handling lifecycle involves the review of alerts, warnings, and suspected events from various sources. In addition, it involves continuous system monitoring and review of risk assessments for systems with high CS incident rates.

Incident Reporting - This phase involves a formal acknowledgement by the incident handler that a CS incident has occurred and that notification of all personnel responsible for responding to, acting upon, or resolving an incident have been notified.

Incident Response – The process of acting upon known identified incidents. The process includes analysis of how the incident occurred, actions to contain the incident, eradicate the cause of the incident, repair the damage, and recover from the incident. This phase includes collection and preparation of a lessons learned report and assistance in the development of an incident report.

Incident Tracking – The process and requirement for State of Kansas and its entities to maintain comprehensive records of all incidents from the time of declaration through closure. The state and its entities are required to track incidents and report the status of those incidents periodically to the Enterprise Security Officer, and the Kansas IT Security Council.

Intrusion – An unauthorized, inappropriate or illegal activity by insiders or outsiders that can be considered a penetration of a system.

Intruder - A person who is the perpetrator of a computer security incident. Intruders are often referred to as “hackers” or “crackers.” Hackers are highly technical experts who penetrated computer systems; the term crackers refers to the experts with the ability to “crack” computer systems and security barriers. Most of the time “cracker” is used to refer to more notorious intruders and computer criminals. An intruder is a vandal who may be operating from within the KANWIN network or attacking from the outside.

Level of Consequence - The impact an incident has on an organization. Impact includes loss of data; the cost to a Kansas state entity or mission area; negative consequences to the organization (e.g. damage to reputation); and the magnitude of damage that must be corrected.

Malicious Code – Also known as “Malware” (malicious software), is a computer code or program designed to deny, destroy, modify, or impede a system’s configuration, programs, data files, or routines. Malicious code comes in several forms, including viruses and worms.

Misuse - Unauthorized use of an account, computer, or network by an intruder or malicious user (or insider).

Need-to-Know - The necessity for access to, knowledge of, or possession of classified or other sensitive information in order to carry out officially sanctioned duties. Responsibility for determining whether a person’s duties require possession or access to this information rests upon the individual having current possession (or ownership) of the information involved, and not upon the prospective recipient.

Pharming – An exploit of the Domain Name Server (DNS) that tries to or actually transforms the legitimate host name into another IP address. The "pharmer" sets up a website looking similar to a legitimate site and harvests personal information from unsuspecting users. Also known as "DNS cache poisoning."

Phishing – An exploit that imitates legitimate companies' emails to entice people to reveal sensitive or private information, or creates a replica of an existing web page to fool a user into submitting personal, financial or password data.

Rootkit – A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.

Spyware - Any technology that aids in gathering information about a person or organization without their knowledge. Sometimes this software is called a "spybot" or "tracking software." Spyware is put in someone's computer to secretly gather information about the user, entity or company and relay it to advertisers, foreign governments, and other interested parties. Spyware can be installed as part of a virus, worm, or result from installation of a program. Spyware is often installed without the user's consent as a drive-by download, by clicking on some option of a deceptive pop-up or webpage, adware or email attachment.

Threat –A circumstance, condition, or event with the potential to cause harm to personnel and/or network resources in the form of destruction, disclosure, modification of data, DoS, and/or fraud, waste and abuse. The most common security threats are to network systems. Network security threats include impersonation, eavesdropping, DoS, packet replay/modification.

Trojan Horse – A non-self-replicating program that seems to have a useful purpose, but in reality has a different malicious purpose.

State of Kansas Organization – Any state entity, or group responsible for purchasing, installing and managing IT resources.

Virus – A small piece of malicious code that attaches itself to another program. It does not run on its own, but executes when the host program is run.

Worm – A type of malicious code that acts as an independent program, and can usually replicate itself without human interaction from one system to another.

Appendix A

Computer Security Incident Response Form

Incident No.	Related/Associated Incident No.
Reported BY:	Phone No.
Date Reported:	Time Reported:
Entity:	Device Type:
Who Was Affected:	Location/Address of Problem:
User Description of Problem:	

The below items are to be filled out by the ESO.	
Incident Type (choose only one)	
Electronic User Compromise ☐ Compromised/Stolen/Altered Data ☐ Theft and use of Others ID's ☐ Other	*Web Site Defacement* ☐ Defacement of Web Site(s) ☐ Redirected Web Site(s) ☐ Other
Denial of Service ☐ Denial of Service ☐ Other	*Reconnaissance Activity* ☐ Probes/Scans ☐ Unauthorized Monitoring ☐ Other
Misuse of Resources ☐ Unauthorized Use of Remote Control ☐ Unauthorized Use of Software ☐ Inappropriate Use of Email ☐ Inappropriate Use of State Resources ☐ Unauthorized Solicitation ☐ Illegal Log-in Attempt ☐ Hoaxes ☐ Storage and/or Distribution of illegal Software ☐ Other	*Malicious Code Activity* ☐ Worm ☐ Virus ☐ Trojan Horse ☐ Root Kits ☐ Other
	Internet Complaint: Describe:
Criticality Classification level	**Sensitivity Classification level**

Physical	*An Alert was sent to:*
☐ Unauthorized Access ☐ Access Control Avoidance ☐ Equipment Stolen or Damaged ☐ Tornado/Storm ☐ Fire ☐ Floods ☐ Bomb Threats ☐ Bio/Chemical Hazards ☐ Other	☐ ITAB Security Contacts ☐ Computer Security Information Officer ☐ State Entity CIO's ☐ Computer Incident Response Team ☐ Technical User Group ☐ E-Mail Administrators ☐ Other: ☐ Legal ☐ Attorney Gen. ☐ D of A Legal ☐ Law enforcement ☐ KBI ☐ Local _____

Who Investigated it:	Evidence Collected (choose) ☐ YES ☐ NO
Number of Intruders:	Number of Hosts:
Incident Source:	Target:
Monetary damage (estimate)	
Analysis of Findings:	
Recommended Action:	
Ticket Closed Date:	By: